



VERIFICATION

I, Ko SASAKI, a national of Japan, Nitto International Patent Office P.P.C., No. 17 Arai Building, 3-3, Shinkawa 1-Chome, Chuo-ku, Tokyo 104-0033, Japan, verify that to the best of my knowledge and belief the following is a true translation made by me of the annexed document which is Japanese Patent Application No. 2000-286479 filed on September 21, 2000.

Dated this 26th day of April, 2005

A handwritten signature in black ink, appearing to read "Ko SASAKI".

Ko SASAKI (Translator)



[NAME OF DOCUMENT] SPECIFICATION

[TITLE OF THE INVENTION]

INFORMATION STORAGE SYSTEM,

INFORMATION TRANSFER SYSTEM AND STORAGE MEDIUM THEREOF

5 [CLAIMS]

[Claim 1] A storage medium comprising:

a storage device for storing information, an encryption key required for encoding, and encoded information;

10 an input/output device for inputting and outputting information stored in said storage device, said encryption key, and encoded information; and

an encoding device for encoding of information and decoding of encoded information,

15 wherein when outputting information stored inside said storage device to outside said storage medium, along with obtaining information encoded by using said encryption key, said encryption key used when encoding information is encoded by using another encryption key thereby to obtain an encoded encryption key, and both said encoded information and encoded encryption 20 key information are output.

[Claim 2] A storage medium comprising:

a storage device for storing information, an encryption key required for encoding, and encoded information;

25 an input/output device for inputting and outputting information stored in said storage device, said encryption key,

and encoding information; and

an encoding device for encoding of information and decoding
of encoded information,

wherein when outputting information stored inside said
5 storage device to outside said storage device, along with
obtaining information encoded by using said encryption key, said
encryption key used when encoding information is encoded by using
another encryption key thereby to obtain an encoded encryption
key, and first, only said encoded information is output, and
10 when a signal showing encoded information was input is input
from an external apparatus, said encoded encryption key is output
after voiding said information stored in said storage device.

[Claim 3] A storage medium according to claim 1 or 2, wherein
said input/output device, said encoding device, and said storage
15 device are constituted on the same semiconductor chip.

[Claim 4] An information storage system comprising,

a storage medium having: a storage device for storing
information, an encryption key required for encoding, and encoded
information; an input/output device for inputting and outputting
20 said information, said encryption key, and encoding information
stored in said storage device; and an encoding device for encoding
of information and decoding of encoded information, and

an external apparatus connected to said storage medium,
wherein information encoded by utilizing an encryption
25 key, and an encryption key utilized when encoding said information,

are sent with an encryption key encoded utilizing another encryption key and stored in said external apparatus.

[Claim 5] An information transfer system comprising,

5 a storage medium having: a storage device for storing information, an encryption key required for encoding, and encoded information; an input/output device for inputting and outputting information stored in said storage device, said encryption key, and encoding information; and an encoding device for encoding of information and decoding of encoded information, and
10 an external apparatus to receive information stored in said storage medium;

wherein when transferring said information to said external apparatus, said encoded information encoded by utilizing an encryption key is sent to said external apparatus, 15 and after a signal showing said encoded information was received is received from said external apparatus, said information stored in said storage device is voided, and an encoded encryption key is sent to an external apparatus.

[DETAILED DESCRIPTION OF THE INVENTION]

20 [0001]

[Field of the Invention]

The present invention relates to an information storage system, information transfer system and to a storage medium utilized in those systems for distributing information on a 25 semiconductor storage medium, and relates in particular to a

method for preventing illegal copying while storing information of high added value onto general information storage mediums such as large capacity magnetic storage in personal computers not having a function to prevent copying of information, and 5 to a method for transferring the same information between storage mediums without copying.

[0002]

[Prior Art(s)]

One method of the related art for distributing information 10 with high added value while preventing illegal copying is a system disclosed in unexamined Japanese Patent publication No. 2000-90039. A brief explanation of the operation of the device is given while referring to FIG. 9.

A block diagram showing a system for preventing 15 unauthorized use by copying is shown in FIG. 9. In the system in FIG. 9, a music server 903 and a client 902 are connected by an Internet 901. A public key and a secret key are made based on the characteristic ID of the playback equipment 911, by the client 902. The public key is sent from a personal computer 910 20 to a server 903 and registered (stored). The secret key is retained in a playback equipment 911. The client 902 makes a request to the server 903 for distribution of the music data. Encryption with the registered public key is performed for music data extracted from a music data base 922. The encrypted music data 25 is sent to the client 902 and stored in the playback equipment

911. During play, the music data is decrypted with the secret key held in the playback equipment 911 while being played. The music data stored in the playback equipment 911 was encrypted with a key made based on the unique ID of the playback equipment 911 and therefore cannot be played back on other playback equipment.

5 [0003]

Another method for transferring information with high added value is disclosed in unexamined Japanese Patent 10 publication No. H11-259964. The operation of the device is briefly described while referring to FIG. 10.

A flowchart of the information transfer system of the related art is shown in FIG. 10. In this device, when data is copied by transfer to the transfer destination, the playing back 15 of the transfer source data is prohibited. A unique identifier is set beforehand into the device at the transfer destination. In step 1050, when the transfer source device is connected to the transfer destination device, an identifier is sent from transfer destination device in step 1051. In step 1052, a search 20 is made in the (pre-registered) identifier control table for the identifier that was sent, and in step 1053 whether or not this identifier was found is determined. If not found, the process shifts to step 1061 and transfer is prohibited. In step 1053, if the identifier is found, a song is selected in step 1054, 25 and a transfer command is made. Next, in step 1055, the data

to be transferred is searched for from the data control table at the transfer source, and the flag is checked in step 1056. If the flag is a "1" in step 1057, then the process shifts to step 1061 and transfer of that data is prohibited since transfer 5 has already occurred. If the flag is a "0", then the data is transferred in step 1058, and in step 1059 the data control table is rewritten.

[0004]

[Problem(s) to be Solved by the Invention]

10 The related art had the problem that imparting added (unique) value to information was difficult since information stored on a semiconductor storage medium was easily copied onto another semiconductor storage medium. Stated conversely, in order to prevent information of high added (unique) value from 15 being easily copied this information was not distributed by semiconductor storage mediums.

In a method of the related art to distribute information of high added (unique) value while preventing illegal use by copying, the server 903 encoded the information of high added 20 (unique) value based on the unique ID of the playback equipment 911 so that listening in on the communication system path and illegally using the same information could be prevented.

[0005]

When passing encoded information from the transfer source 25 device to the transfer destination device, a two-step combination,

of "Encoding and transferring unique (added) value information such as music data by means of a common key encoding method." and "Encoding and sending the common key used for encoding by the public key encoding method." was generally used on account 5 of the processing speed and simple key management. Since in the latter encoding, an encoding key capable of being decoded at the transfer destination device was utilized (keys were shared), information of significant value could be utilized at the transfer destination device.

10 [0006]

In the method of the related art, for transferring information of high added (unique) value without copying the information between storage mediums, the transfer of data could be achieved by data copy permit/prohibit flags, and by installing 15 a function to prohibit data at the data transfer source after copying the data. However, in both of these methods of the related art, the communication path for information between the transfer source and the transfer destination was not adequately protected and information of high added (unique) value could be illegally 20 acquired by intercepting (listening in) information on the same communication path. Further, This procedure has a point when usable data was present at the data transfer source and the data transfer destination, so the data at data transfer source and the data transfer destination were both capable of being utilized 25 due to an interruption in communications between the data transfer

source and the transfer destination.

[0007]

In order to resolve the problems of the related art, it is therefore an object of the present invention to provide a storage medium and information processing technology utilizing that storage medium capable of outputting information stored in the storage medium in a format unusable by other information devices or storage mediums (not sharing data encryption and key) by adding functions to the storage medium itself.

It is a further object of the present invention to provide a storage medium and information processing technology utilizing that storage medium capable of transferring information stored on the storage medium rather than copying the information so that the uniqueness of the information is always assured, and copying of the information by interception on the communication path is prevented.

[0008]

[Means for Solving the Problem(s)]

To achieve the above mentioned objects of the invention, in a first aspect of the invention, a storage medium is comprised of a storage device for storing information, an encryption key required for encoding, and encoded information; an input/output device for inputting and outputting information stored in the storage device, the encryption key, and encoding information; and an encoding device for encoding of information and decoding

of encoded information. When outputting information stored inside the storage device to outside the storage medium, along with obtaining information encoded by using the encryption key, the encryption key used when encoding information is encoded 5 by using another encryption key thereby to obtain an encoded encryption key, and both the encoded information and encoded encryption key are output.

[0009]

In a second aspect of the invention, a storage medium is 10 comprised of a storage device for storing information, an encryption key required for encoding, and encoded information; an input/output device for inputting and outputting information stored in the storage device, the encryption key, and encoded information; and an encoding device for encoding of information 15 and decoding of encoded information. When outputting information stored inside the storage device to outside the storage medium, along with obtaining information encoded by using the encryption key, the encryption key used when encoding information is encoded by using another encryption key thereby 20 to obtain an encoded encryption key, and first, only the encoded information is output, and when a signal showing encoded information was input is input from an external apparatus, the encoded encryption key is output after voiding the information stored in the storage device.

25 [0010]

In the first and second aspects of the invention, the input/output device, the encoding device, and the storage device are constituted on the same semiconductor chip.

[0011]

5 In a third aspect of the invention, an information storage system has a storage medium comprised of a storage device for storing information, an encryption key required for encoding, and encoded information; an input/output device for inputting and outputting information the encryption key, and encoding 10 information stored in the storage device; and an encoding device for encoding of information and decoding of encoded information; and an external apparatus connected to the storage medium. Information encoded by utilizing an encryption key, and an encryption key utilized when encoding the information, are sent 15 with an encryption key encoded utilizing another encryption key and stored in the external apparatus.

[0012]

In a fourth aspect of the invention, an information transfer system has a storage medium comprised of a storage device for 20 storing information, an encryption key required for encoding, and encoded information; an input/output device for inputting and outputting information stored in the storage device, the encryption key, and encoding information; and an encoding device for encoding of information and decoding of encoded information; 25 and an external apparatus to receive information stored in the

storage medium. When transferring the information to the external apparatus, the encoded information encoded by utilizing an encryption key is sent to the external apparatus, and after a signal showing the encoded information was received is received 5 from the external apparatus, the information stored in the storage device is voided, and the encryption key is sent to the encoded external apparatus.

[0013]

[Embodiment(s) of the Invention]

10 Hereafter, the embodiments of the present invention are described while referring to the accompanying work drawings.

FIG. 1 is a block diagram showing an overview of the embodiment of the information processing system for the present invention. As shown in FIG. 1, the information processing system 15 is comprised of an information creator and information generating device 101, an information distributing device 103 connected by way of a transfer means 102, at least one dedicated information processing device 105 unit connected by a communications line 104 with the information distributing device 103, at least one 20 semiconductor storage medium 110 unit, and at least one information reproducing device 109 unit.

[0014]

Aside from the dedicated information processing device 105, a general-purpose information processing device 106 such 25 as a personal computer comprised of a semiconductor storage medium

access means 107, and information reproducing device 108 may also be provided.

Information is generated by the information creator and the information generating device 101 and stored in the 5 information distributing device 103. A communication line may also be used at this time for transferring information, or information may also be sent by a magnetic storage medium such as a floppy disk. The information distributing device 103 processes the information or adds supplemental information 10 according to the request from the dedicated information processing device 105, general-purpose information processing device 106 or information reproducing device 108 and sends the information by way of the communication line 104.

[0015]

15 The dedicated information processing device 105, general-purpose information processing device 106 and information reproducing device 108 transfer the information to the connected semiconductor storage medium 110. The dedicated information processing device 105 accumulates a plurality of 20 information and may also process the information or add supplemental information. The general-purpose information processing device 106 and the information reproducing device 108 send the information transferred from the information distributing device 103 basically unchanged to the semiconductor 25 storage medium 110. Information is exchanged at this time between

the information distributing device 103 and dedicated information processing device 105, between the dedicated information processing device 105 and semiconductor storage medium 110, and between the information distributing device 103 and semiconductor storage medium 110 for mutual recognition and authentication of the other device.

5 [0016]

The semiconductor storage medium 110 stored with distributed information added with the processed or supplemental 10 information, is connected to the information reproducing device 109, and sends the stored information at the request of the information reproducing device 109. Information is exchanged at this time between the information reproducing device 109 and semiconductor storage medium 110 for mutual recognition and 15 authentication.

15 [0017]

Methods for safely distributing information generated by the information creator to the semiconductor storage medium 110 are not dealt with in particular by the present invention, the 20 distributed information is assumed to be stored in the semiconductor storage medium 110.

[0018]

The first embodiment of the present invention is described while referring to FIG. 2 through FIG. 4, and FIG. 8.

25 FIG. 2 is a block diagram showing the first embodiment

of the storage medium of the present invention. The semiconductor storage medium 110 is mainly comprised of an encoding device 210, a storage device 211, and as an I/F device 212. In FIG. 2, the encoding device 210 is comprised of an asymmetrical key encoder 206 for encoding by using a method with a different encoding key and a decoding key and referred to as an asymmetrical key code and public key code; a symmetrical key encoder 204 for encoding by a coding method using an encoding key and decoding key that are the same and called a symmetrical key code and common key code; and a symmetrical key generator 204 using some kind of random number generating process. A storage device 211 stores an information 201, symmetrical key 203, first asymmetrical key 205a, second asymmetrical key 205b, symmetrical key 208 encoded with the first asymmetrical key, and encoded information 207 encoded with the symmetrical key. An interface device 212 (hereafter called I/F device) controls the exchange of information between the semiconductor 110 and an external apparatus. A data bus 213 is used to exchange information and control signals between the encoding device 210, a storage device 211 and an I/F device 212. The data bus 209 is used to exchange information and control signals between the semiconductor storage medium 110 and the external apparatus.

[0019]

The semiconductor storage medium 110 is recorded beforehand with the information peculiar to the storage medium.

In other words, the first asymmetrical key 205a and second asymmetrical key 205b unique to the semiconductor storage medium 110 are stored in the storage device 211. One method that may be used for setting the unique information is to write it onto the semiconductor storage medium 110 during the manufacturing stage, so that the unique information cannot be easily rewritten when the semiconductor storage medium 110 has been completed. Another method that may be used is to set the unique information after the semiconductor storage medium 110 has been completed, utilizing a method known by the persons where information is sufficiently controlled and restricted, e.g. a production supervisor.

[0020]

The first and second asymmetrical keys 205a and 205b of semiconductor storage medium 110 are key data of a method referred to as asymmetrical key encoding and public key encoding. In the encoding method called asymmetrical key encoding and public key encoding, when a text is encoded with the first asymmetrical key and an encoded text generated, the encoded text can then only be decoded using the second asymmetrical key as the decoding key. Further, when a text is encoded with the second asymmetrical key as the encoding key and an encoded text generated, the encoded text can then only be decoded using the first asymmetrical key as the decoding key. Hereafter, the first asymmetrical key will be treated as the public key and the second asymmetrical key

treated as the secret key. The reference numeral 207 signifies the encoded information encoded with utilizing the symmetrical key, and the reference numeral 208 signifies the encoded symmetrical key which is encoded utilizing the first asymmetrical 5 key.

[0021]

Next, the process in this embodiment for transferring information 201 stored in the semiconductor storage medium 110 into the general-purpose information processing device 106 and 10 the semiconductor storage medium access means 107 is described next while referring to FIG. 3 and FIG. 8A.

FIG. 3 is a drawing showing the first embodiment of the information transfer function from the storage medium of the information transfer system of the present invention. FIG. 8A 15 and B are flowcharts for describing the operation of the information transfer system of FIG. 3. FIG. 8A shows the operation for transferring information from the semiconductor storage medium 110. FIG. 8B shows the information transfer to the semiconductor storage medium 110.

20 [0022]

The semiconductor storage medium 110 performs the following operation in response to a transmit request for information 201 from the general-purpose information processing device 106 and the semiconductor storage medium access means 25 107 connected to the semiconductor storage medium 110.

[0023]

5 In describing the operation while referring to FIG. 2, FIG. 3 and FIG. 8, in step 202 a random number is generated by the function of the encoding device 210 in the semiconductor storage medium 110. The generated random number is utilized as the symmetrical key 203 to encode the information 201. In step 204a, the information 201 is symmetrically encoded with the symmetrical key 203 by the function of the encoding device 210, and the encoded information 207 is generated.

10 On the other hand, the symmetrical key 203 on the other hand, is asymmetrically encoded with a first asymmetrical key 205a as the encoding key, by the functioning of the encoding device 210 and the encoded symmetrical key 208 is generated.

[0024]

15 The encoded information 207 and the encoded symmetrical key 208 generated in the above procedure are sent in step 209a to the general-purpose information processing device 106 and semiconductor storage medium access means 107 by the function of the IF device 212. The encoded information 207 and the encoded 20 symmetrical key 208 can in this way be stored for backup in the general-purpose information processing device 106 and semiconductor storage medium access means 107.

[0025]

25 The encoded information 207 transferred to the general-purpose information processing device 106 and

semiconductor storage medium access means 107 by means of the above procedure, cannot be decoded without the symmetrical key 203. The encoded symmetrical key 208 cannot correctly be decoded without the second asymmetrical key 205b. Here, the second 5 asymmetrical key 205b is unique key data of the semiconductor storage medium 110, and is unobtainable by the general-purpose information processing device 106 and semiconductor storage medium access means 107. The general-purpose information processing device 106 and semiconductor storage medium access means 107 therefore cannot decode the symmetrical key 208 and 10 cannot use the information 201.

[0026]

In other words, even if a copy of the information was made by the general-purpose information processing device 106, after 15 the information 201 stored in the semiconductor storage medium 110 is transferred to the general-purpose information processing device 106 and semiconductor storage medium access means 107, the copy of the encoded information 207 is incapable of being used on the general-purpose information processing device 106 and semiconductor storage medium access means 107, so that 20 unlimited copying of the information 201 by the general-purpose information processing device 106 can in this way prevented.

[0027]

Or, the symmetrical key 203 used for encoding the 25 information 201 to be transferred is indispensable for decoding

the encoded information 207, so essentially each (piece of) information to be transferred should be controlled and stored in the semiconductor storage medium 110, however the semiconductor storage medium 110 uses the unique information 5 of the first asymmetrical key 205a to make the symmetrical key 203 into an encoded symmetrical key 208, and send it outside the semiconductor storage medium 110 along with the encoded information 207 in step 209a. Control and storage of a plurality of symmetrical keys is therefore not required in the semiconductor 10 storage medium 110 so that only the first and second asymmetrical key pair 205a and 205b need to be controlled and stored. In other words, this brings the advantage that along with easy control of the keys, the storage capacity of the storage device 211 is not taken up by a plurality of symmetrical key data.

15 [0028]

Next, the process for transferring the encoded information 207 that was sent to the general-purpose information processing device 106 and semiconductor storage medium access means 107 according to the procedure shown in FIG. 3, to the semiconductor 20 storage medium 110 is next explained while referring to FIG. 4 and FIG. 8B.

[0029]

FIG. 4 is a drawing showing the first embodiment of the information transfer function to the storage medium of the 25 information transfer system of the present invention.

In response to a transfer request from the general-purpose information processing device 106 and semiconductor storage medium access means 107 connected to the semiconductor storage medium 110, the following operations are performed by the 5 semiconductor storage medium 110. In step 209b, the semiconductor storage medium 110 inputs the encoded information 207 and encoded symmetrical key 208 from the general-purpose information processing device 106 and semiconductor storage medium access means 107 by the function of the I/F device 212. The semiconductor 10 storage medium 110 next in step 206b uses the second asymmetrical key 205b as the decoding key by means of the function of the encoding device 210 and performs asymmetrical decoding of the encoded symmetrical key 208, obtaining the symmetrical key 203. Further, in step 204b, the symmetrical key 203 obtained by the 15 functioning of encoding device 210, is used as a decoding key to perform symmetrical decoding of the encoded information 207, and the information 201 is obtained.

[0030]

Herein, the second asymmetrical key 205b is unique key 20 data of the semiconductor storage medium 110 so that the encoded information 207 sent to the general-purpose information processing device 106 and semiconductor storage medium access means 107 can only be decoded in the semiconductor storage medium 110 which is the transmission source of the encoded information 25 207. The encoded information 207 sent to the general-purpose

information processing device 106 and semiconductor storage medium access means 107 is therefore impossible to be decoded and used in a semiconductor storage medium other than the semiconductor storage medium 110 which is the transmission source 5 of the transferred encoded information 207 so that unconditional copying of the information 201 can in this way be prevented.

[0031]

As was mentioned above, the semiconductor storage medium of this embodiment encodes communication data between devices 10 to prevent their unauthorized use by eavesdropping on the communication path, and when information is transferred from a source device to a destination device, that encoding can be performed in a two step key combination of, "Encode and transfer unique (added) value information such as music data." and "Use 15 another key to encode and transfer that key used encoding." However, since a decoding key utilized in the latter part of the combination is impossible (not a shared key) to decode the encoded key at the transfer destination device, the decoding and use of valuable encoded information by the transfer 20 destination device is assured to be impossible, and that information can only be utilized by returning and writing that same information in the transfer source device. Using a fixed key for encoding unique (high added value) information would present problems in terms of security since a fixed code can 25 provide a significant advantage to parties trying to decode the

encoded information so that keys required are made by pseudo-random number generators when encoded communications are required. The transfer source device outputs the key generated for encoding unique (high added value) information, along with 5 the encoded unique (high added value) information encoded in a format only decodable by the transfer source device so that key management is simple (control only of unique keys) and further, the storage capacity is not constricted by a plurality of key information.

10 [0032]

In other words, while also preventing the unauthorized use of high added value information by copying, the semiconductor storage medium of the present embodiment is also capable of storing unique (high added value) information in for example, 15 large capacity magnetic storage devices for personal computers, in particular, general-purpose information storage mediums not incorporating a function to prevent the illegal copy of information.

[0033]

20 Next, the second embodiment of the present invention is described next while referring to FIG. 5 and FIG. 6. Here, FIG. 5 is an overall block diagram of the information control and transfer system of the present invention, and FIG. 6 is a flowchart showing the operation of the second embodiment of the information 25 transfer system of the present invention.

FIG. 5 shows an overall structure consisting of the semiconductor storage medium 110a and 110b, and the same device to control them (dedicated information processing device 105, general-purpose information processing device 106 and 5 semiconductor storage medium access means 107 or information reproducing device 108) of the present embodiment.

[0034]

In FIG., the information 201, a symmetrical key generator 202, symmetrical key 203, symmetrical key encoder 204, a 10 symmetrical key encoder 206, data bus 209, encoding device 210, storage device 211, I/F device 212 and the data bus 231 are identical to the first embodiment.

[0035]

A reference numeral 110a denotes the semiconductor storage 15 medium forming the transfer source, 110b is the semiconductor storage medium forming the transfer destination.

A reference numeral 205a denotes the public key (hereafter, first asymmetrical key) utilized in the asymmetrical encoding method of the information transfer destination semiconductor 20 storage medium 110b, and stored beforehand in the storage device 211 of information transfer source semiconductor storage medium 110a. A reference numeral 205b denotes the secret key (hereafter, second asymmetrical key) utilized in the asymmetrical encoding method of the information transfer destination semiconductor 25 storage medium 110b, and stored beforehand in the storage medium

211 of information transfer destination semiconductor storage medium 110b.

[0036]

The reference numerals 501a and 501b denote the interface devices (hereafter I/F device) controlling the exchange of information and control signals between the dedicated information processing device 105, general-purpose information processing device 106 and semiconductor storage medium access means 107, or information reproducing device 108.

10 [0037]

A reference numerals 502 denotes a control circuit controlling the input of information by way of one I/F device 501a so as to be output by another I/F device 501b.

Reference numerals 503a and 503b are reference numerals 15 denoting data buses for exchanging information and control signals between the I/F device 501a and the control device 502.

[0038]

Next, the procedure when transferring the information 201 stored in the information transfer source semiconductor storage medium 110a to the information transfer destination semiconductor storage medium 110b by way of the dedicated information processing device 105, general-purpose information processing device 106 and semiconductor storage medium access means 107, or information reproducing device 108 is described 25 next while referring to FIG. 6.

[0039]

At the request for transfer of information 201 by way of the dedicated information processing device 105, general-purpose information processing device 106 and 5 semiconductor storage medium access means 107, or information reproducing device 108 connected to the information transfer source semiconductor storage medium 110a, the information transfer source semiconductor storage medium 110a and the information transfer destination semiconductor storage medium 10 110b perform the following operation.

[0040]

In step 601 in FIG. 6, the information transfer source semiconductor storage medium 110a generates a symmetrical key. In other words, it generates a random number by the function 15 of the encoding device 210, and this generated random number is utilized as the symmetrical key 203 for encoding the information 201. In step 602, the information 201 is encoded the symmetrical key 203 by the function of the encoding device 210 and the encoded information 207 is generated.

20 The encoded information 207 generated in the above procedure is transmitted in step 603a to the information transfer destination semiconductor storage medium 110b by way of the dedicated information processing device 105, general-purpose information processing device 106 and semiconductor storage 25 medium access means 107, or the information reproducing device

108 by means of the functioning of the I/F device 212.

[0041]

The information transfer destination semiconductor storage medium 110b, receives the encoded information 207 in step 603b, and in step 604 checks the received encoded information 207 for transmission errors. If errors are present, then the information transfer destination semiconductor storage medium 110b sends an information retransmission request to the information transfer source semiconductor storage medium 110a in step 605a. In step 605b, the information transfer source semiconductor storage medium 110a receives the information retransmission request, and in step 603a sends the encoded information again. If there are no transmission errors, the information transfer destination semiconductor storage medium 110b in step 606a sends an information receive completion notification to the information transfer source semiconductor storage medium 110a.

[0042]

The information transfer source semiconductor storage medium 110a receives the information receive completion notification in step 606b, and deletes the information 201 in step 607. Regarding this information deletion, if data access from an external source by way of the I/F device 212 can be guaranteed to be impossible, then the actual deletion of data from the storage device 211 need not be performed.

[0043]

Next, in step 608, the information transfer source semiconductor storage medium 110a uses the functions of the encoding device 210 to perform asymmetrical encoding of the 5 symmetrical key 203 using the first asymmetrical key 205a as the encoding key, and generates the encoded symmetrical key 208.

[0044]

The encoded symmetrical key 208 generated in the above procedure, is sent in step 609a to the information transfer 10 destination semiconductor storage medium 110b by way of the dedicated information processing device 105, or general-purpose information processing device 106 and semiconductor storage medium access means 107, or the information reproducing device 108 by means of the functioning of the I/F device 212.

15 The information transfer destination semiconductor storage medium 110b, receives the encoded symmetrical key 208 in step 609b, and in step 610 checks the received encoded symmetrical key 208 for transmission errors. If errors are present, then the information transfer destination semiconductor storage 20 medium 110b sends an information retransmission request to the information transfer source semiconductor storage medium 110a in step 611a. In step 611b the information transfer source semiconductor storage medium 110a receives the encoded symmetrical key retransmission request, and returning to step 25 609a once again sends the encoded symmetrical key. If there are

no transmission errors, the information transfer destination semiconductor storage medium 110b in step 612 performs asymmetrical decoding of the encoded symmetrical key 208 using the asymmetrical key 205b as the coding key, and generates the 5 symmetrical key 203. Next, in step 613, the information transfer destination semiconductor storage medium 110b performs symmetrical decoding of the encoded information 207 with the symmetrical key 203 as the coding key, and generates the information 201.

10 [0045]

The encoded information 207 output from the information transfer source semiconductor storage medium 110a in the above procedure, cannot be correctly decoded without the symmetrical key 203. Also, the encoded symmetrical key 208 cannot correctly 15 perform decoding without the second asymmetrical key 205b. Here, the second asymmetrical key 205b is unique data of the information transfer destination semiconductor storage medium 110b and cannot be obtained without the same device. Therefore, devices on the same communication path as the encoded information 207, 20 such as the dedicated information processing device 105, or general-purpose information processing device 106 and semiconductor storage medium access means 107, or the information reproducing device 108 cannot decode the encoded symmetrical key 208 and utilize the information 201.

25 [0046]

Or, in the process for transferring data between the information transfer source semiconductor storage medium 110a and the information transfer destination semiconductor storage medium 110b, the information 201 present within the information transfer source semiconductor storage medium 110a is voided (step 5 607) in between the point that the encoded information 207 is sent and the point that the encoded symmetrical key 208 is sent, so that there is no period in which the information 201 is present in both the information transfer source semiconductor storage 10 medium 110a and information transfer destination semiconductor storage medium 110b devices. In this way, at the point that transfer of encoded information 207 is complete, rights to hold the information 203 shifted from the information transfer source semiconductor storage medium 110a to the information transfer 15 destination semiconductor storage medium 110b. After that, transferring of encoded symmetrical key 208 is only possible for semiconductor storage medium 110

[0047]

In other words, even if communications end abnormally due 20 to a communications error or malicious communication interruption at any point in the data transfer process between the information transfer source semiconductor storage medium 110a and the information transfer destination semiconductor storage medium 110b, it can be assured to be totally impossible 25 for both the information transfer source semiconductor storage

medium 110a and the information transfer destination semiconductor storage medium 110b to utilize the information 203.

[0048]

5 However, the example in the present embodiment showed the case of transferring data between a plurality of storage media, however data transfer is not necessarily limited to a plurality 10 of storage media and data transfer may for example also be implemented between devices other than storage media such as between the dedicated information processing device 105 and the storage medium 110 based on the same procedure, or data transfer may also be implemented in a plurality of storage medium, for example, by way of a plurality of information reproducing devices 109 or a plurality of dedicated information processors 105.

15 [0049]

Also in the above embodiments, a transmission error check of the received encoded information (step 604) or a transmission error check of the encoded symmetrical key (step 610) was implemented for the encoded information transmission (step 603a, 20 603b) or the transmission of encoded information keys (step 609a, 609b), however the transmission error check process (step 604 or step 610) may be omitted, and the information reception completion transmission processing (step 606a, 606b) may be performed immediately after receiving the encoded information 25 or the asymmetrical key decoding (step 612) processing may be

performed immediately after receiving the encoded symmetrical key 208 when the communication reliability of the data bus 209 between the semiconductor storage medium 110a and 110b is high.

[0050]

5 As was mentioned in the example described for the semiconductor storage medium in the present embodiment, the transfer of information 201 is possible between a plurality of semiconductor storage mediums 110a and 110b. The inability to simultaneously use the same information 201 on the plurality 10 of semiconductor storage mediums 110a and 110b is also guaranteed. In other words, in the semiconductor storage mediums of the present embodiment, a combination of encoded communications and precise processing of transactions provides a semiconductor medium that allows information movement between storage mediums 15 while preventing the unauthorized use by copying of information of high added value.

[0051]

In the first and second embodiments, the encoding may be implemented by dedicated hardware within the encoding device 210, or may be implemented by a CPU within that equipment and software processing. A storage area for key information and work area needed for encoding may be provided solely within the encoding device 210, or the storage device 211 may be utilized.

[0052]

25 Also the example in the first and second embodiments used

a symmetrical key encoding method in the encoding of the information 201, and an asymmetrical key encoding method in the encoding of the symmetrical key 203 however the invention is not limited by this example, and if a two-step structure of 5 information encoding and encoding of the encoding key is usable, and further if a key to encode that same encoding key can be peculiar to the medium and can be held in secret in the medium, then an optional combination of encoding method, symmetrical key encoding method, and asymmetrical encoding method may be 10 used.

[0053]

The semiconductor storage medium 110 (or 110a, 110b) is installed with an encoding device 212, as well as an I/F device 212 and a storage device 211 having the essential functions of 15 a storage medium. In a structure where the semiconductor storage medium 110 performs all data exchange with external apparatus only by way of an I/F device 212, and also by forming for example, a structure where the storage device 211, I/F device 212 and the encoding device 212 are on the same semiconductor wafer, 20 direct external access to the data bus 213 connected between these devices is impossible. In this way, the information 201 stored in the storage device 211 of the semiconductor storage medium 110, and the key information 203, 205a, 205b necessary 25 for encoding, are protected from unauthorized access and the tamper-proofing is enhanced.

[0054]

Also, in the implementation of the semiconductor storage medium 110 shown in the first and second embodiments, the storage device 211 may be a flash memory, and the encoding device 210 and I/F device 212 may be on the same wafer which constitutes a semiconductor chip, sealed for example in the package of the size of a stamp or a credit card. A semiconductor storage medium 110 of the above configuration can serve as an information distribution medium and will prove beneficial and convenient to the user for using information of high added value in the information processing system as shown in FIG. 1.

[0055]

Or, the first and second embodiments shows a semiconductor storage medium utilizing some manner of semiconductor storage device as the storage device 211. However, this invention is not necessarily limited to a semiconductor storage medium and for example, no problem will arise from use of a magnetic storage medium utilizing a magnetic storage device as the storage device. In such a case for example, by forming the encoding device 210, I/F device 212 and access means to the magnetic storage device on the same semiconductor wafer, access to the data bus 213 from outside the storage medium 110 can be prevented.

[0056]

Or, in the first and second embodiments, the semiconductor storage medium 110 had the configuration shown in FIG. 2 or FIG.

5. However the semiconductor storage medium 110 may have the configuration shown in FIG. 7.

[0057]

5 FIG. 7 is a overall block diagram showing another embodiment of the semiconductor storage medium. FIG. 7 can be utilized in the examples of the first and second embodiments.

In this figure, structural elements identical to the same elements in FIG. 2 or FIG. 5 have the same reference numerals and their explanation is omitted here.

10 In this figure, reference numeral 212a denotes a data interface device (hereafter data I/F device) for controlling the usual exchange of data and control signals between the semiconductor storage medium 110 and external apparatus. The reference numeral 212b denotes a data interface device (hereafter 15 secure data I/F device) for safely controlling the exchange of data and control signals to be exchanged between the semiconductor storage medium 110 and external apparatus.

[0058]

20 The reference numeral 209c denotes a data bus for the normal exchange of data and control signals between the semiconductor storage medium 110 and external apparatus. The reference numeral 209d denotes a secure data bus for safely controlling the exchange of data and control signals to be exchanged between the semiconductor storage medium 110 and external apparatus.

25 A plurality of I/F devices are physically separated as

seen from outside the storage medium 110, and for example the setting of the first asymmetrical key 205a and second asymmetrical key 205b into the storage device 211, and though the methods are not related in detail here, recognition procedures such as 5 between the storage medium 110 and external equipment, and the exchange of data important for the security of the system are performed by the secure data I/F device 212b. Tasks that not particularly vital such as transmission and receiving of encoded information 207, are performed by way of the data I/F device 10 212a.

[0059]

With the structure mentioned above, by providing a plurality of physically separate data I/F in the storage medium 110, in the above structure, a protocol and bus configuration 15 for the exchange of information particularly vital in terms of security can be provided that are not dependent on the exchange of ordinary information.

[0060]

As was explained in the above, in the invention as described, 20 the system comprised of a creator of information or information generating device, information distributing device, communications line to distribute information, semiconductor storage medium, terminal to write information in that semiconductor storage medium connected with the communications 25 line, and information reproducing device to reproduction

information stored in the semiconductor storage medium in a state separated from the communications line; the uniqueness of the information can be assured by providing a storage medium and information processing system utilizing that storage medium 5 capable of outputting information stored on a storage medium in a format unusable by other information devices or storage media; along with the capability to move rather than copy the information stored in the storage medium.

[0061]

10 In this way, data of high added value can be safely distributed by the semiconductor storage medium, and applications such as for information distribution services are possible.

[0062]

15 [Effect of the Invention]

The present invention, as was explained above, is capable of outputting information stored on a storage medium in a format unusable by other information devices or storage media. The uniqueness of the information can be assured by moving the 20 information stored in the storage medium rather than copying the information. Data of high added value can in this way be safely distributed by the semiconductor storage medium, and applications such as to information distribution services become possible.

25 [Brief Description of the Drawings]

[FIG. 1]

It is a block diagram showing an overview of the embodiment of the information processing system of the present invention.

[FIG. 2]

5 It is a block diagram showing the first embodiment of the storage medium of the present invention.

[FIG. 3]

10 It is a drawing showing the first embodiment of the information transfer function from the storage medium of the information transfer system of the present invention.

[FIG. 4]

15 It is a drawing showing the first embodiment of the information transfer function for information transfer to the storage medium of the information transfer system of the present invention.

[FIG. 5]

It is an overall block diagram of the information control and transfer system of the present invention.

[FIG. 6]

20 It is a flowchart showing the operation of the second embodiment of the information transfer system of the present invention.

[FIG. 7]

25 It is an overall block diagram showing another embodiment of the semiconductor storage medium.

[FIG. 8]

It is a flowchart for describing the operation of the information transfer system of FIG. 3.

[FIG. 9]

5 It is a block diagram showing the system of the related art to prevent unauthorized use by copying.

[FIG. 10]

It is a flowchart of the information transfer system of the related art.

10 [Explanation of Marks]

101...information generating device, 102...transfer means,
103...information distributing device, 104...communications line,

105...one dedicated information processing device,

106...general-purpose information processing device,

15 107...semiconductor storage medium access means, 108...information reproducing device, 109...information reproducing device,

110...semiconductor storage medium, 201...information,

202...symmetrical key generating step, 203...symmetrical key,

204...symmetrical key encoding step, 204a...symmetrical key

20 encoding step, 204b...symmetrical key decoding step, 205a...first asymmetrical key, 205b...second asymmetrical key,

206...asymmetrical key encoding step, 206a...asymmetrical key

encoding step, 206b...asymmetrical key decoding step, 207...encoded

information, 208...encoded symmetrical key, 209...data bus,

25 209a...transmission of encoded information and encoded

symmetrical key, 209b...receipt of encoded information and encoded symmetrical key, 209c...data bus, 209d...secure data bus, 210...encoding device, 211...storage device, 212...I/F device, 212a...data I/F device, 212b...secure data I/F device, 501a...I/F device, 501b...I/F device, 502...control circuit (device), 503a...data bus, 503b...data bus, 601...symmetrical key generating step, 602...symmetrical key encoding step, 603a...transmission of encoded information, 603b...receipt of encoded information, 604...checking step on transmission error of encoded information 10 key, 605a...transmission of request of re-transmission of information, 605b...receipt of request of re-transmission of information, 606a...transmission of completion on receiving information, 606b...receipt of completion on receiving information, 607...deleting step of information, 608...asymmetrical key encoding step, 609a...transmission of encoded symmetrical key, 609a...receipt of encoded symmetrical key, 610...checking step on transmission error of encoded symmetrical key, 611a...transmission of request of re-transmission of symmetrical key, 611b...receipt of request of re-transmission of symmetrical key, 612...asymmetrical key decoding step, 613...symmetrical key decoding step, 901...network, 902...client, 903...music distributor server, 910...personal computer, 911...headphone stereo for mobile phone, 922...music database.

[Name of Document] ABSTRACT

[Abstract]

[Problem] A storage medium and an information processing system utilizing that storage medium capable of outputting information 5 stored on the storage medium in a format unusable by other information devices or storage mediums. A storage medium and an information processing system utilizing that storage medium further capable of transferring information stored on the storage medium rather than copying the information so that the uniqueness 10 of the information is assured.

[Means for Solving] A storage medium comprised of a storage device for storing information, information required for encryption and encrypted information, and an I/F device for inputting and outputting information, information required for 15 coding and store encrypted information in a storage device or from an external apparatus other than the storage device, and an encoding device for coding of information and decoding of encoded information. When outputting information stored inside the storage device to outside the storage medium, information 20 is encoded using encryption key information, and along with obtaining the encoded information and obtaining the encoded encryption key information by using another encryption information, both the encoded information and encoded encryption key information are output so that decoding the information 25 without the storage medium is impossible.

[Selected Drawing] Fig. 2



FIG. 1

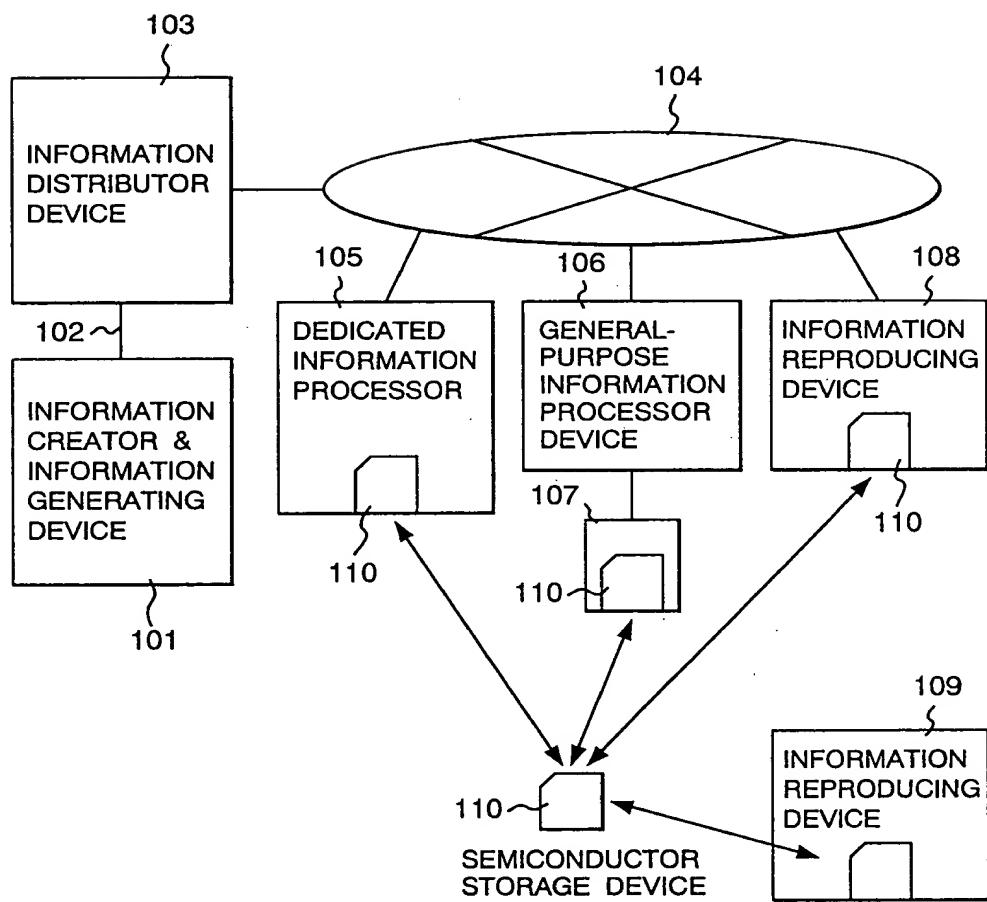
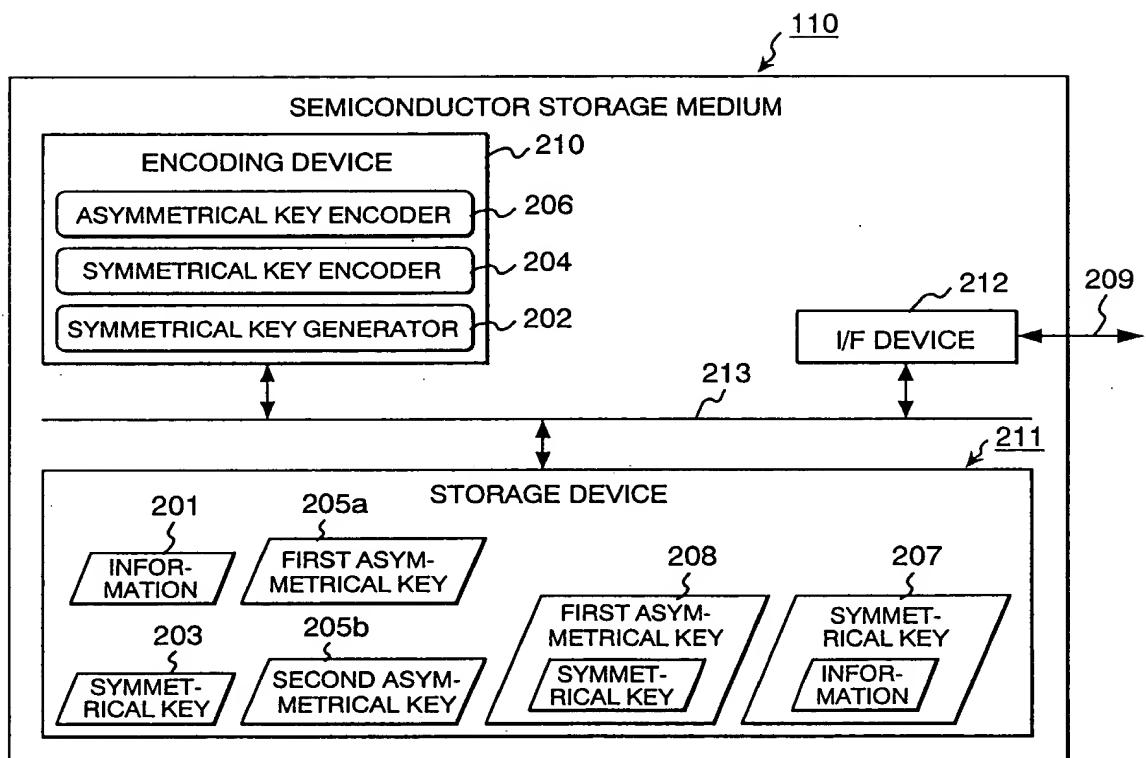


FIG. 2





3/10

FIG. 3

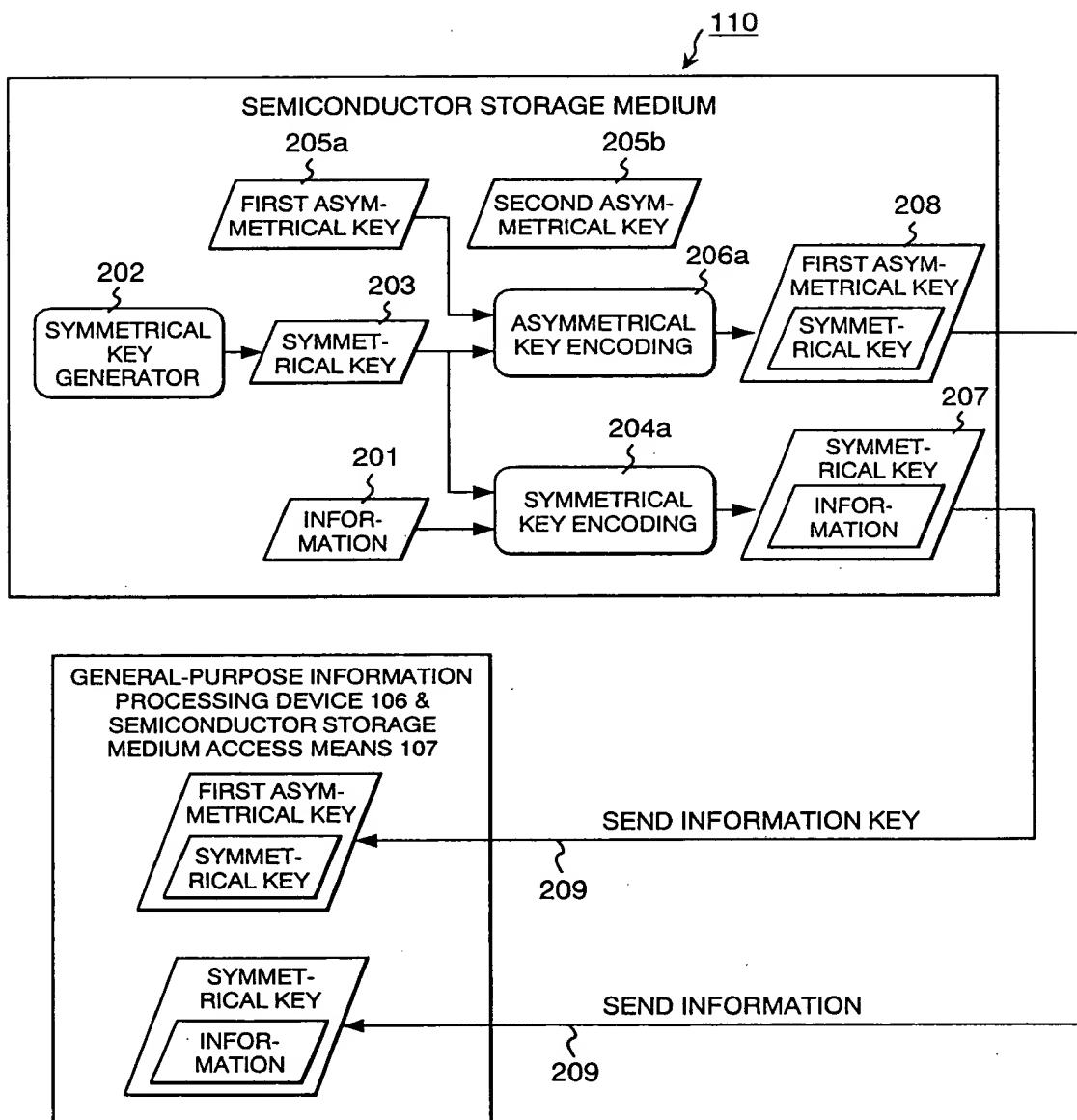




FIG. 4

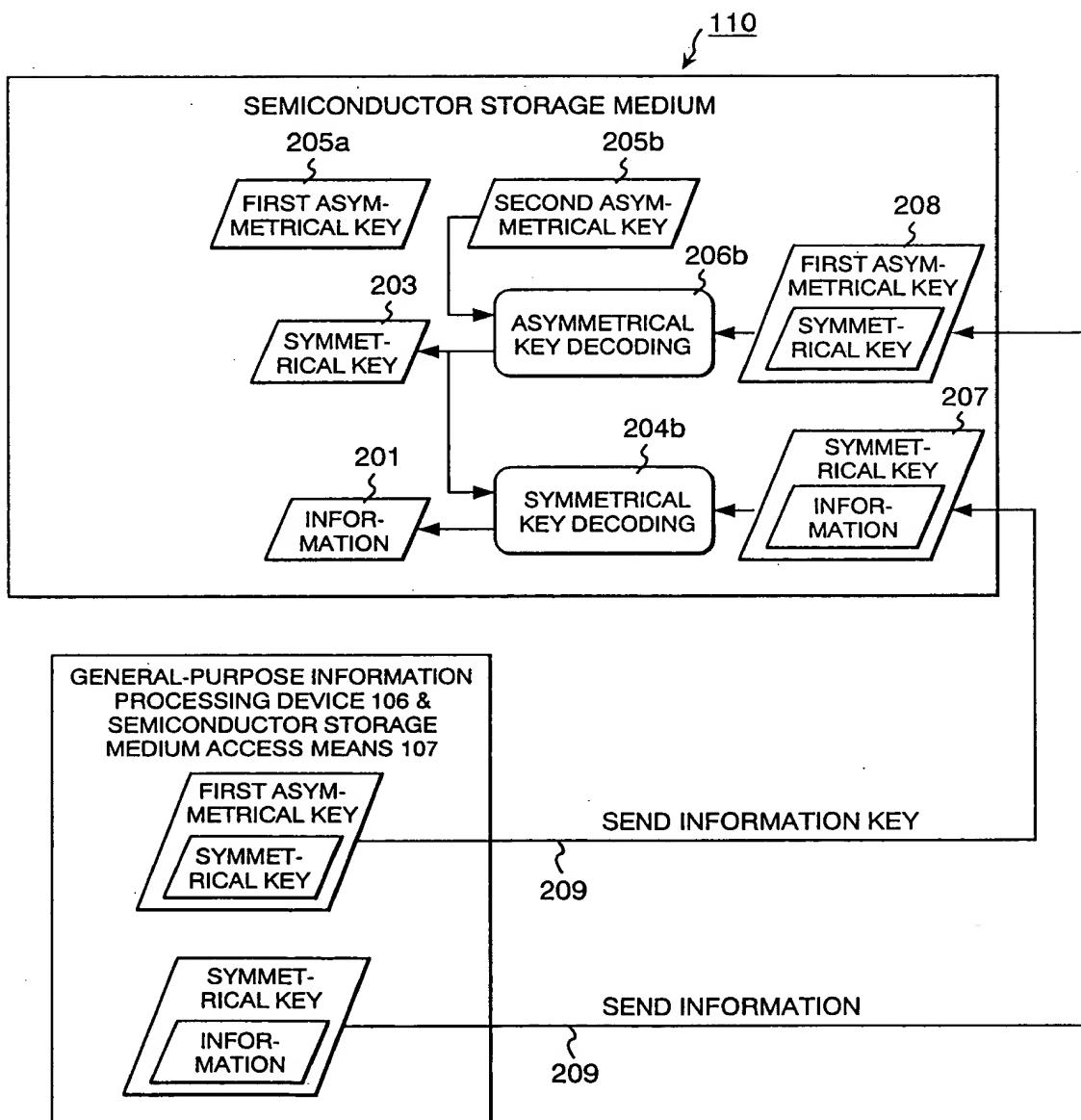




FIG. 5

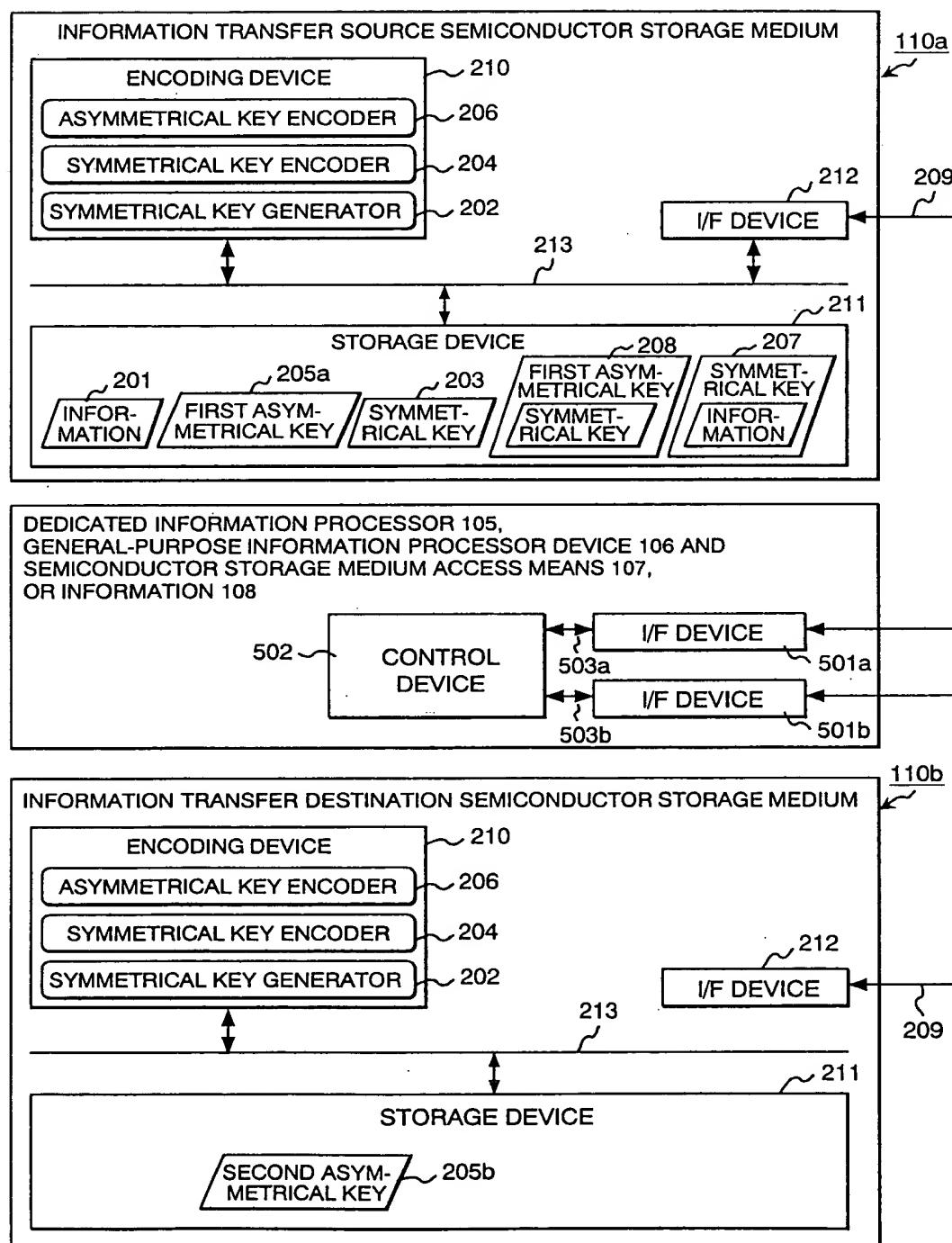




FIG. 6

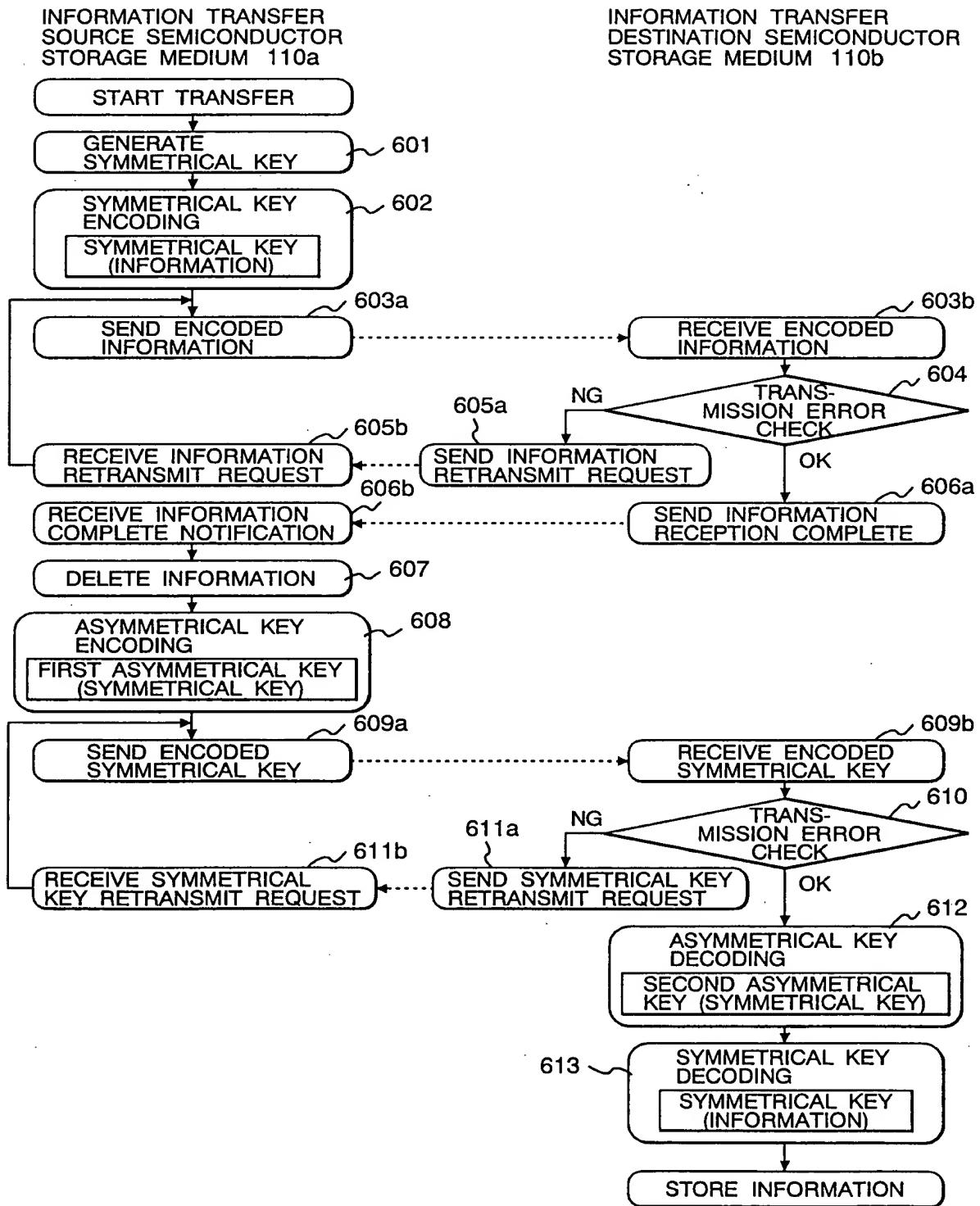
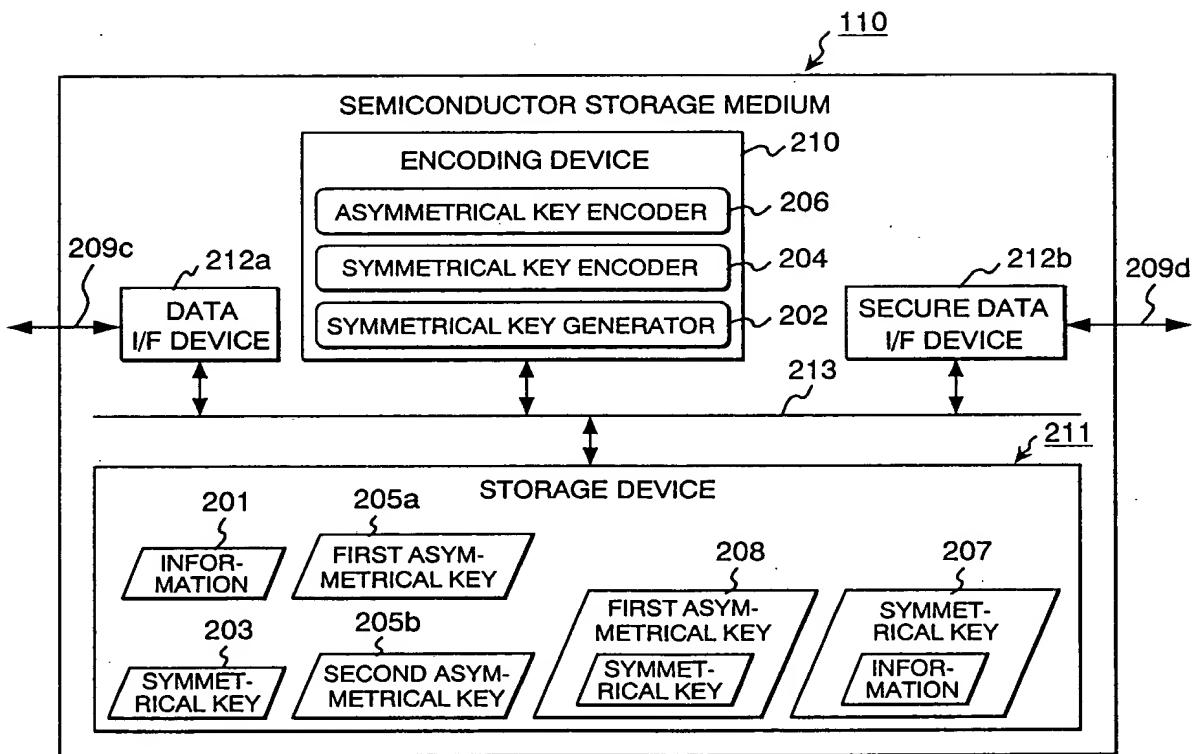




FIG. 7



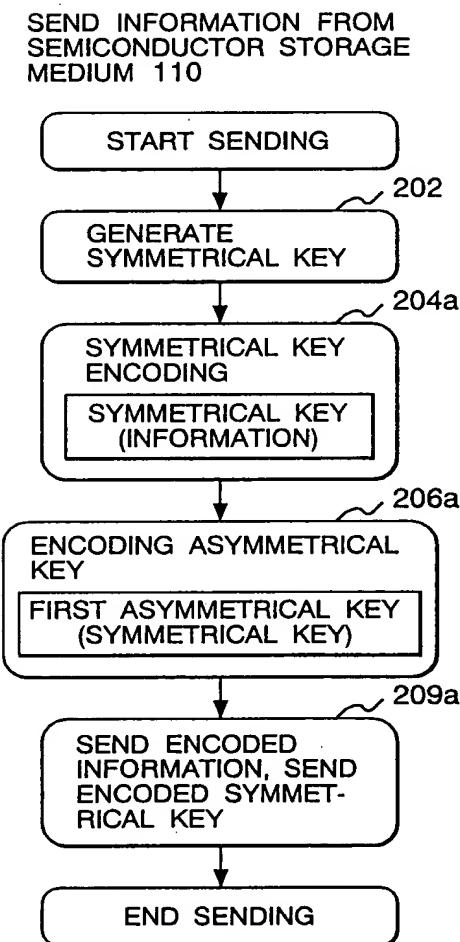
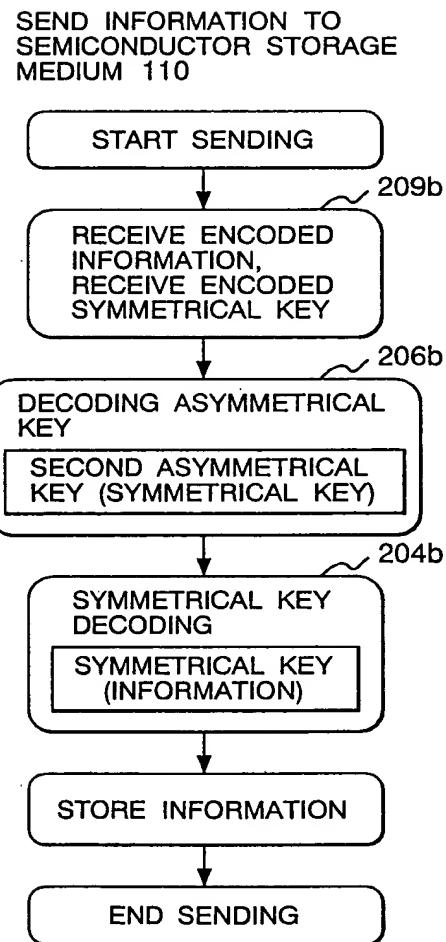
**FIG. 8A****FIG. 8B**

FIG. 9

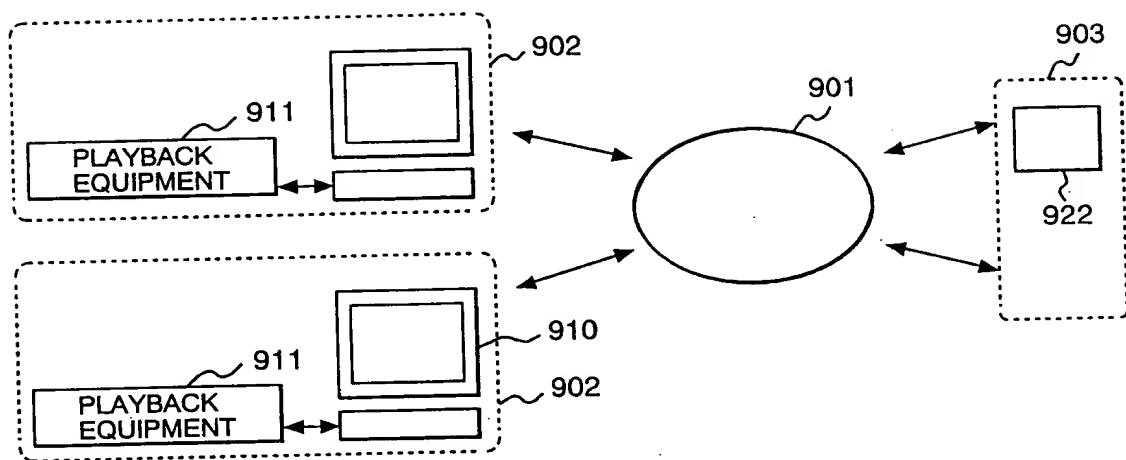




FIG. 10

